

Defining Quantum Control Flow

Mingsheng Ying, Nengkun Yu and Yuan Feng

QCIS, FEIT, University of Technology, Sydney, Australia

and

TNList, Dept. of CS, Tsinghua University, China

Email: Mingsheng.Ying@uts.edu.au, yingmsh@tsinghua.edu.cn

Abstract

A remarkable difference between quantum and classical programs is that the control flow of the former can be either classical or quantum. One of the key issues in the theory of quantum programming languages is defining and understanding quantum control flow. A functional language with quantum control flow was defined by Altenkirch and Grattage [*Proc. LICS'05*, pp. 249-258]. This paper extends their work, and we introduce a general quantum control structure by defining three new quantum program constructs, namely quantum guarded command, quantum choice and quantum recursion. We clarify the relation between quantum choices and probabilistic choices. An interesting difference between quantum recursions with classical control flows and with quantum control flows is revealed.

1 Introduction

Since Knill [8] introduced the Quantum Random Access Machine (QRAM) model for quantum computing and proposed a set of conventions for writing quantum pseudocodes in 1996, several quantum programming languages have been defined in the last 16 years; for example QCL by Ömer [12], qGCL by Sanders and Zuliani [13], QPL by Selinger [14], and see [7] for an excellent survey. One of the key design ideas of almost all existing quantum languages can be summarised by the influential slogan “quantum data, classical control” proposed by Selinger [14], meaning that the control flow of a quantum program is still classical, but the program operates on quantum data. An exception is Altenkirch and Grattage’s functional language QML [2], where “quantum control” flow was introduced; more precisely, they observed that in the quantum setting the case construct naturally splits into two variants:

- **case**, which measures a qubit in the data it analyses;
- **case^o**, which analyses quantum data without measuring.

The control flow in the **case** construct is determined by the outcome of a measurement and thus is classical. However, a quantum control flow appears in the **case^o** construct, as shown

in the following example where a special form of the case° , namely the $\text{if}^\circ - \text{then} - \text{else}$ statement, is used.

Example 1.1 *Basic quantum gates implemented in QML [2]: The Hadamard gate is written as:*

$$\begin{aligned} \text{had} &: \mathbf{Q}_2 \multimap \mathbf{Q}_2 \\ \text{had } x &= \text{if}^\circ x \\ &\quad \text{then } \left\{ \frac{1}{\sqrt{2}}(\text{qfalse} - \text{qtrue}) \right\} \\ &\quad \text{else } \left\{ \frac{1}{\sqrt{2}}(\text{qfalse} + \text{qtrue}) \right\} \end{aligned}$$

and the CNOT gate is as follows:

$$\begin{aligned} \text{cnot} &: \mathbf{Q}_2 \multimap \mathbf{Q}_2 \multimap \mathbf{Q}_2 \otimes \mathbf{Q}_2 \\ \text{cnot } c \ x &= \text{if}^\circ c \\ &\quad \text{then } (\text{qtrue}, \text{not } x) \\ &\quad \text{else } (\text{qfalse}, x) \end{aligned}$$

where \mathbf{Q}_2 is the type of qubits, and not is the NOT gate:

$$\begin{aligned} \text{not} &: \mathbf{Q}_2 \multimap \mathbf{Q}_2 \\ \text{not } x &= \text{if}^\circ x \\ &\quad \text{then } \text{qfalse} \\ &\quad \text{else } \text{qtrue} \end{aligned}$$

A new research line of quantum programming with quantum control flow was then initiated by Altenkirch and Grattage in [2] and further pursued by themselves and others in a series of papers [3, 9].

The present paper continues this line of research, and we extend the idea of “quantum control” by introducing three new quantum program constructs:

(1) Quantum Guarded Command: Our first step toward a general quantum control structure is to introduce a quantum generalisation of Dijkstra’s guarded command [6]. Recall that a guarded command can be written as follows:

$$\Box_{i=1}^n b_i \rightarrow C_i \tag{1}$$

where for each $1 \leq i \leq n$, the command C_i is guarded by the Boolean expression b_i , and C_i will be executed only when b_i is true. Obviously, the case operator in QML is a quantum generalisation of guarded command with classical control. On the other hand, as shown in the above example, the case° operator in QML implements a unitary transformation by decomposing it into two orthogonal branches along the quantum control flow determined by a chosen qubit. So, it is already a kind of guarded command with quantum control flow.

An even clearer idea for defining quantum guarded command stems from a quite different area, namely quantum walks [4], [1]:

Example 1.2 *Quantum walks on graphs [1]: Let (V, E) be an n -regular directed graph. Then we can label each edge with a number between 1 and n such that for each $1 \leq i \leq n$, the directed edges labeled i form a permutation. Let \mathcal{H}_V be the Hilbert space spanned by states $\{|v\rangle\}_{v \in V}$. Then for each $1 \leq i \leq n$, we can define a shift operator S_i on \mathcal{H}_V :*

$$S_i|v\rangle = |\text{the } i\text{th neighbour of } v\rangle$$

for any $v \in V$. We introduce an auxiliary quantum variable q with the state Hilbert space \mathcal{H}_q spanned by $\{|i\rangle\}_{i=1}^n$. Now we are able to combine the operators S_i ($1 \leq i \leq n$) along q to form a whole shift operator:

$$S \triangleq \square_{i=1}^n q, |i\rangle \rightarrow S_i \quad (2)$$

on $\mathcal{H}_q \otimes \mathcal{H}_V$:

$$S|v, i\rangle = (S_i|v\rangle)|i\rangle \quad (3)$$

for any $1 \leq i \leq n$ and $v \in V$. If we further choose a unitary operator U on \mathcal{H}_q then a coined quantum walk on graph (V, E) is defined by modelling its single step by the unitary operator:

$$W \triangleq S(I_{\mathcal{H}_V} \otimes U)$$

on $\mathcal{H}_V \otimes \mathcal{H}_q$, where $I_{\mathcal{H}_V}$ is the identity operator in \mathcal{H}_V . Usually, \mathcal{H}_q is called the “coin space”, and U the “coin-tossing operator”.

The guarded command notation is adopted in Eq. (2) to indicate that the shift operator S is indeed a guarded command with quantum control. It is interesting to note that both Examples 1.1 and 1.2 defined a guarded command with quantum control, but their defining strategies are quite different: in Example 1.1, a quantum control flow is *detected* by decomposing a unitary operator along an *existing* qubit; in contrast, a quantum control flow is *created* in Example 1.2 by introducing a *new* quantum variable so that we can combining a family of unitary operators along the created flow. The defining strategy used in Example 1.2 naturally leads us to a general form of quantum guarded command:

$$\square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i \quad (4)$$

where P_1, \dots, P_n are a family of quantum programs, and a new family of quantum variables \bar{q} that do not appear in P_1, \dots, P_n is introduced so that we can form a quantum guarded command by combining P_1, \dots, P_n along an orthonormal basis $\{|i\rangle\}$ of the state space of \bar{q} . For each $1 \leq i \leq n$, P_i is guarded by the basis state $|i\rangle$, and a superposition of these basis states yields a quantum control flow.

(2) Quantum Choice: Guarded commands are the most widely accepted mechanism for nondeterministic programming. Nondeterminism in guarded command (1) is a consequence of the “overlapping” of the guards b_1, \dots, b_n . In particular, if $b_1 = \dots = b_n = \text{true}$, then guarded command (1) becomes a demonic choice:

$$\square_{i=1}^n C_i, \quad (5)$$

where the alternatives C_i are chosen unpredictably. Usually, the demonic choice is separately defined as an explicit operator rather than a special case of guarded command due to its importance as a means of abstraction in programming.

To formalise randomised algorithms, research on probabilistic programming [10] started in 1980's with the introduction of probabilistic choice:

$$\Box_{i=1}^n C_i @ p_i, \quad (6)$$

where $\{p_i\}$ is a probability distribution; that is, $p_i \geq 0$ for all i , and $\sum_{i=1}^n p_i = 1$. The probabilistic choice (6) randomly chooses the command C_i with probability p_i for every i , and thus it can be seen as a refinement of the demonic choice (5). A probabilistic choice is often used to represent a decision in forks according to a certain probability distribution in a randomised algorithm.

A natural question then arises in the realm of quantum programming: is it possible to define a quantum choice of programs? Indeed, an idea is already there in the construction of quantum walks, although not explicitly stated. In Example 1.2, each shift operator S_i can be considered as an independent program, the “coin-tossing operator” U is employed to create a superposition of S_i ($1 \leq i \leq n$), and thus the single step operator W can be seen as a quantum choice among S_i ($1 \leq i \leq n$). Extending the idea used in Example 1.2, we can define a general quantum choice as a sequential composition of a “coin-tossing” program and a quantum guarded command:

$$\Box_{i=1}^n P; \bar{q}, |i\rangle \rightarrow P_i \triangleq P; \Box_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i, \quad (7)$$

where P_1, \dots, P_n are a family of quantum programs, \bar{q} is a new family of quantum variables with $\{|i\rangle\}$ as an orthonormal basis of its state space, and P is a quantum program acting on \bar{q} . Intuitively, quantum choice (7) first runs program P to produce a superposition of the execution paths of programs P_i ($1 \leq i \leq n$), and then the guarded command $\Box_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i$ follows. During the execution of the guarded command, each P_i is running along its own path within the whole superposition of execution paths of P_i ($1 \leq i \leq n$). It is widely accepted that quantum superposition is responsible for the advantage of quantum computers over classical computers. The power of superposition of quantum states has been successfully exploited in quantum computing. Quantum choices may provide a platform for explore a higher level of quantum superposition in computing, namely the superposition of quantum programs.

(3) Quantum Recursion: Most classical programming languages allow direct specification of recursive procedures. Quantum loops and more general quantum recursive procedures were already defined in Selinger's language QPL [14], and termination of quantum loops were analysed by the authors in [18]. But quantum recursions considered in [14, 18] contain no quantum control flows because their branchings in quantum programs are all determined by the outcomes of quantum measurements. After introducing quantum guarded commands and quantum choices, loops and recursive procedures with quantum control flows can be defined. As will be seen later, a major difference between quantum recursions with and without quantum controls is: auxiliary quantum variables must be introduced in order to define quantum controls. Thus, localisation mechanism is needed in defining quantum recursions with quantum control so that consistency of quantum variables is guaranteed.

1.1 Technical Contributions of the Paper

As shown above, a general notion of quantum control flow comes naturally out from generalising the case° construct in Altenkirch and Grattage’s language QML and the shift operators in quantum walks. However, a major difficulty arises in defining the semantics of quantum guarded commands. For the case where no quantum measurement occur in any P_i ($1 \leq i \leq n$), the semantics of each P_i is simply a sequence of unitary operators, and the semantics of guarded command (4) can be defined in exactly the same way as Eq. (3). Whenever some P_i contains quantum measurements, however, its semantic structure becomes a tree of linear operators with branching happening at the points where measurements are performed. Then defining the semantics of guarded command (4) requires to properly combine a collection of trees such that certain quantum mechanical principles are obeyed. This problem will be circumvented in Sec. 3.

1.2 Organisation of the Paper

A new quantum programming language QGCL with quantum guarded commands is defined in Sec. 2. Sec. 3 prepares some key ingredients needed in defining the semantics of QGCL. The denotational semantics and weakest precondition semantics of QGCL are presented in Sec. 4. In Sec. 5, quantum choice is defined in terms of quantum guarded command, and probabilistic choice is implemented by quantum choice by introducing local variables. Because of the limited space, quantum recursion is only briefly touched in Sec. 6. For readability, all proofs are deferred to the Appendix.

2 QGCL: A Language with Quantum Guarded Commands

We now define a quantum programming language QGCL with quantum guarded commands. QGCL is essentially an extension of Sanders and Zuliani’s qGCL obtained by adding quantum control flow. But the presentation of QGCL is quite different from qGCL due to the complications in the semantics of quantum guarded commands. We assume a countable set $qVar$ of quantum variables ranged over by q, q_1, q_2, \dots . For simplicity of the presentation, we only consider a purely quantum programming language, but we include a countably infinite set Var of classical variables ranged over by x, y, \dots so that we can use them to record outcomes of quantum measurements. However, classical computation described by, for example, the assignment statement $x := e$ in a classical programming language is excluded. It is required that the sets of classical and quantum variables are disjoint. For each classical variable $x \in Var$, its type is assumed to be a non-empty set D_x ; that is, x takes values from D_x . For each quantum variable $q \in qVar$, its type is a Hilbert space $type(q) = \mathcal{H}_q$, which is the state space of the quantum system denoted by q . For a sequence $\bar{q} = q_1, q_2, \dots$ of quantum variables, we write:

$$type(\bar{q}) = \mathcal{H}_{\bar{q}} = \bigotimes_{i \geq 1} \mathcal{H}_{q_i}.$$

Similarly, for any set $V \subseteq qVar$, we write:

$$type(V) = \mathcal{H}_V = \bigotimes_{q \in V} \mathcal{H}_q.$$

In particular, we write \mathcal{H}_{all} for $type(qVar)$. To simplify the notation, we often identify a sequence of variables with the set of these variables provided they are distinct.

Definition 2.1 *For each QGCL program P , we write $var(P)$ for the set of its classical variables and $qvar(P)$ for its quantum variables. QGCL programs are inductively defined as follows:*

1. **abort** and **skip** are programs, and

$$var(\mathbf{abort}) = var(\mathbf{skip}) = \emptyset,$$

$$qvar(\mathbf{abort}) = qvar(\mathbf{skip}) = \emptyset.$$

2. If $\bar{q} = q_1, \dots, q_k$ is a sequence of quantum variables, and U is a unitary operator on $type(\bar{q})$, then $U[\bar{q}]$ is a program, and

$$var(U[\bar{q}]) = \emptyset, \quad qvar(U[\bar{q}]) = \bar{q}.$$

3. If $\bar{q} = q_1, \dots, q_k$ is a sequence of quantum variables, x is a classical variable, $M = \{M_m\}$ is a quantum measurement in $type(\bar{q})$, and $\{P_m\}$ is a family of programs indexed by the outcomes m of measurement M such that $spec(M) \subseteq D_x$, where $spec(M) = \{m\}$ is the spectrum of M ; that is, the set of all possible outcomes of M , and $x \notin \bigcup_m var(P_m)$, then

$$P \triangleq M[x \leftarrow \bar{q}] : \{P_m\} \tag{8}$$

is a program, and

$$var(P) = \{x\} \cup \bigcup_m var(P_m),$$

$$qvar(P) = \bar{q} \cup \bigcup_m qvar(P_m).$$

4. If $\bar{q} = q_1, \dots, q_k$ is a sequence of quantum variables, $\{|i\rangle\}_{i=1}^n$ is an orthonormal basis of $type(\bar{q})$, and $\{P_i\}_{i=1}^n$ is a family of programs such that

$$\bar{q} \cap \bigcup_{i=1}^n qvar(P_i) = \emptyset,$$

then

$$P \triangleq \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i$$

is a program, and

$$\begin{aligned} \text{var}(P) &= \bigcup_{i=1}^n \text{var}(P_i), \\ \text{qvar}(P) &= \bar{q} \cup \bigcup_{i=1}^n \text{qvar}(P_i). \end{aligned}$$

5. If P_1 and P_2 are programs such that $\text{var}(P_1) \cap \text{var}(P_2) = \emptyset$, then $P_1; P_2$ is a program, and

$$\begin{aligned} \text{var}(P_1; P_2) &= \text{var}(P_1) \cup \text{var}(P_2), \\ \text{qvar}(P_1; P_2) &= \text{qvar}(P_1) \cup \text{qvar}(P_2). \end{aligned}$$

The meanings of **abort** and **skip** are the same as in a classical programming language. Two kinds of statements are introduced in the above definition to describe basic quantum operations, namely unitary transformation and measurement. In the unitary transformation $U[\bar{q}]$, only quantum variables \bar{q} but no classical variables appear, and the transformation is applied to \bar{q} . In statement (8), a measurement M is first performed on quantum variables \bar{q} with the outcome stored in classical variable x , and then whenever outcome m is reported, the corresponding subprogram P_m is executed. The intuitive meaning of quantum guarded command was already carefully explained in Sec. 1. Whenever the sequence \bar{q} of quantum variables can be recognised from the context, $\square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i$ can be abbreviated to $\square_{i=1}^n |i\rangle \rightarrow P_i$. The sequential composition $P_1; P_2$ is similar to that in a classical language, and the requirement $\text{var}(P_1) \cap \text{var}(P_2) = \emptyset$ means that the outcomes of measurements performed at different points are stored in different classical variables. Such a requirement is mainly for technical convenience, and it will considerably simplify the presentation. The syntax of QGCL can be summarised as follows:

$$\begin{aligned} P &:= \mathbf{abort} \mid \mathbf{skip} \mid P_1; P_2 \\ &\mid U[\bar{q}] \quad (\text{unitary transformation}) \\ &\mid \mathbf{measure} M[\bar{q}] : \{P_m\} \quad (\text{quantum measurement} \\ &\quad = \text{classical guarded command}) \\ &\mid \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i \quad (\text{quantum guarded command}) \end{aligned} \tag{9}$$

3 Guarded Compositions of Quantum Operations

3.1 Guarded composition of unitary operators

A major difficulty in defining the semantics of QGCL comes from the treatment of guarded commands where a guarded composition of semantic functions is vital. To ease the understanding of a general definition of such a guarded composition, we start with the guarded composition of unitary operators, which is a straightforward generalisation of the quantum walk shift operator S in Example 1.2.

Definition 3.1 For each $1 \leq i \leq n$, let U_i be an unitary operator in Hilbert space \mathcal{H} . Let \mathcal{H}_s be a Hilbert space with $\{|i\rangle\}$ as an orthonormal basis. Then we define a linear operator:

$$U \triangleq \square_{i=1}^n |i\rangle \rightarrow U_i$$

in $\mathcal{H} \otimes \mathcal{H}_s$ by

$$U(|\psi\rangle|i\rangle) = (U_i|\psi\rangle)|i\rangle$$

for any $|\psi\rangle \in \mathcal{H}$ and for any $1 \leq i \leq n$. Then by linearity we have:

$$U \left(\sum_{i=1}^n |\psi_i\rangle|i\rangle \right) = \sum_{i=1}^n (U_i|\psi_i\rangle)|i\rangle \quad (10)$$

for any $|\psi_1\rangle, \dots, |\psi_n\rangle \in \mathcal{H}$. The operator U is called the guarded composition of U_i ($1 \leq i \leq n$) along $\{|i\rangle\}$.

Example 3.1 *Quantum multiplexor:* As a quantum generalisation of multiplexor, a well-known notion in digit logic, quantum multiplexor (QMUX for short) was introduced in [15] as a useful tool in synthesis of quantum circuits. A QMUX U with k select qubits and d -qubit-wide data bus can be represented by a block-diagonal matrix:

$$U = \text{diag}(U_0, U_1, \dots, U_{2^k-1}) = \begin{pmatrix} U_0 & & & \\ & U_1 & & \\ & & \dots & \\ & & & U_{2^k-1} \end{pmatrix}.$$

Multiplexing $U_0, U_1, \dots, U_{2^k-1}$ with k select qubits is exactly the guarded composition

$$\square_{i=0}^{2^k-1} |i\rangle \rightarrow U_i$$

along the computational basis of k qubits.

Lemma 3.1 The guarded composition $\square_{i=1}^n |i\rangle \rightarrow U_i$ is an unitary operator in $\mathcal{H} \otimes \mathcal{H}_s$.

3.2 Operator-valued functions

For any Hilbert space \mathcal{H} , we write $\mathcal{L}(\mathcal{H})$ for the space of (linear) operators on \mathcal{H} .

Definition 3.2 Let Δ be a nonempty set. Then a function $F : \Delta \rightarrow \mathcal{L}(\mathcal{H})$ is called an operator-valued function in \mathcal{H} over Δ if

$$\sum_{\delta \in \Delta} F(\delta)^\dagger \cdot F(\delta) \sqsubseteq I_{\mathcal{H}}, \quad (11)$$

where $I_{\mathcal{H}}$ is the identity operator in \mathcal{H} , and \sqsubseteq stands for the Löwner order; that is, $A \sqsubseteq B$ if and only if $B - A$ is a positive operator. In particular, F is said to be full when Eq. (11) becomes equality.

The simplest examples of operator-valued function are unitary operators and measurements.

Example 3.2 1. A unitary operator on Hilbert space \mathcal{H} can be seen as a full operator-valued function over a singleton $\Delta = \{\epsilon\}$.

2. A measurement M on Hilbert space \mathcal{H} can be seen as a full operator-valued function over its spectrum $\text{Spec}(M)$.

More generally, a super-operator defines a family of operator-valued functions. Let \mathcal{E} be a super-operator on Hilbert space \mathcal{H} . Then \mathcal{E} has the Kraus operator-sum representation: $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$, meaning: $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ for all density operators ρ in \mathcal{H} . For such a representation, we set $\Delta = \{i\}$ for the set of indexes, and define an operator-valued function over Δ by $F(i) = E_i$ for every i . Since operator-sum representation of \mathcal{E} is not unique, \mathcal{E} defines not only a single operator-valued function. We write $\mathbb{F}(\mathcal{E})$ for the family of operator-valued functions defined by all Kraus operator-sum representations of \mathcal{E} . Conversely, an operator-valued function determines uniquely a super-operator.

Definition 3.3 Let F be an operator-valued function in Hilbert space \mathcal{H} over set Δ . Then F defines a super-operator $\mathcal{E}(F)$ in \mathcal{H} as follows:

$$\mathcal{E}(F) = \sum_{\delta \in \Delta} F(\delta) \circ F(\delta)^\dagger.$$

For a family \mathbb{F} of operator-valued functions, we write $\mathcal{E}(\mathbb{F}) = \{\mathcal{E}(F) : F \in \mathbb{F}\}$. It is obvious that $\mathcal{E}(\mathbb{F}(\mathcal{E})) = \{\mathcal{E}\}$. On the other hand, for any operator-valued function F over $\Delta = \{\delta_1, \dots, \delta_k\}$, Theorem 8.2 in [11] indicates that $\mathbb{F}(\mathcal{E}(F))$ consists of all operator-valued functions G over $\Gamma = \{\gamma_1, \dots, \gamma_l\}$ such that

$$G(\gamma_i) = \sum_{j=1}^n u_{ij} \cdot F(\delta_j)$$

for each $1 \leq i \leq n$, where $n = \max(k, l)$, $U = (u_{ij})$ is an $n \times n$ unitary matrix, $F(\delta_i) = G(\gamma_j) = 0_{\mathcal{H}}$ for all $k+1 < i \leq n$ and $l+1 < j \leq n$.

3.3 Guarded composition of operator-valued functions

We first introduce a notation. Let Δ_i be a nonempty set for every $1 \leq i \leq n$. Then the superposition of Δ_i ($1 \leq i \leq n$) is defined as follows:

$$\bigoplus_{i=1}^n \Delta_i = \{\oplus_{i=1}^n \delta_i : \delta_i \in \Delta_i \text{ for every } 1 \leq i \leq n\}.$$

Definition 3.4 For each $1 \leq i \leq n$, let F_i be an operator-valued function in Hilbert space \mathcal{H} over set Δ_i . Let \mathcal{H}_s be a Hilbert space with $\{|i\rangle\}$ as an orthonormal basis. Then the

guarded composition of F_i ($1 \leq i \leq n$) along $\{|i\rangle\}$ is defined to be the operator-valued function in $\mathcal{H} \otimes \mathcal{H}_s$ over $\bigoplus_{i=1}^n \Delta_i$:

$$F \triangleq \square_{i=1}^n |i\rangle \rightarrow F_i,$$

$$F(\bigoplus_{i=1}^n \delta_i) \left(\sum_{i=1}^n |\psi_i\rangle |i\rangle \right) = \sum_{i=1}^n \left(\prod_{k \neq i} \lambda_{k\delta_k} \right) (F_i(\delta_i) |\psi_i\rangle) |i\rangle \quad (12)$$

for any $|\psi_1\rangle, \dots, |\psi_n\rangle \in \mathcal{H}$ and for any $\delta_i \in \Delta_i$ ($1 \leq i \leq n$), where

$$\lambda_{k\delta_k} = \sqrt{\frac{\text{tr} F_k(\delta_k)^\dagger F_k(\delta_k)}{\sum_{\tau_k \in \Delta_k} \text{tr} F_k(\tau_k)^\dagger F_k(\tau_k)}}. \quad (13)$$

In particular, if F_k is full and $d = \dim \mathcal{H} < \infty$, then

$$\lambda_{k\delta_k} = \sqrt{\frac{\text{tr} F_k(\delta_k)^\dagger F_k(\delta_k)}{d}}$$

for any $\delta_k \in \Delta_k$ ($1 \leq k \leq n$).

It is easy to see that whenever Δ_i is a singleton for all $1 \leq i \leq n$, then Eq. (12) degenerates to Eq. (10). So, the above definition is a generalisation of Definition 3.1.

Example 3.3 (Guarded composition of measurements) We consider two simplest measurements; that is, measurements on a qubit in the computational basis $|0\rangle, |1\rangle$ and in basis $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$:

$$M^0 = \{M_0^0 = |0\rangle\langle 0|, M_1^0 = |1\rangle\langle 1|\},$$

$$M^1 = \{M_0^1 = |+\rangle\langle +|, M_1^1 = |-\rangle\langle -|\}.$$

Then their guarded composition along another qubit is measurement

$$M = (|0\rangle \rightarrow M_0) \square (|1\rangle \rightarrow M_1)$$

$$= \{M_{00}, M_{01}, M_{10}, M_{11}\}$$

on two qubits, where

$$M_{ij}(|\psi_0\rangle|0\rangle + |\psi_1\rangle|1\rangle) = \frac{1}{\sqrt{2}}(M_i^0|\psi_0\rangle|0\rangle + M_j^1|\psi_1\rangle|1\rangle)$$

for any states $|\psi_0\rangle, |\psi_1\rangle$ of a qubit and $i, j \in \{0, 1\}$.

The following lemma shows that the guarded composition of operator-valued functions is well-defined.

Lemma 3.2 The guarded composition $F \triangleq \square_{i=1}^n |i\rangle \rightarrow F_i$ is an operator-valued function in $\mathcal{H} \otimes \mathcal{H}_s$ over $\bigoplus_{i=1}^n \Sigma_i$. In particular, if all F_i ($1 \leq i \leq n$) are full, then so is F .

3.4 Guarded composition of super-operators

Guarded composition of a family of super-operators can be defined through the guarded composition of the operator-valued functions generated from them.

Definition 3.5 For each $1 \leq i \leq n$, let \mathcal{E}_i be a super-operator in Hilbert space \mathcal{H} . Let \mathcal{H}_s be a Hilbert space with $\{|i\rangle\}$ as an orthonormal basis. Then the guarded composition of \mathcal{E}_i ($1 \leq i \leq n$) is defined to be the family of super-operators:

$$\begin{aligned} \square_{i=1}^n |i\rangle \rightarrow \mathcal{E}_i &= \{\mathcal{E}(\square_{i=1}^n |i\rangle \rightarrow F_i) : \\ &F_i \in \mathbb{F}(\mathcal{E}_i) \text{ for every } 1 \leq i \leq n\}. \end{aligned}$$

It is easy to see that if $n = 1$ then the above guarded composition of super-operators consists of only \mathcal{E}_1 . For $n > 1$, however, it is not a singleton, as shown by the following:

Example 3.4 Let \mathcal{E}_0 and \mathcal{E}_1 be the super-operators in Hilbert space \mathcal{H} defined by unitary operators U_0, U_1 , respectively; that is, $\mathcal{E}_i = U_i \circ U_i^\dagger$ ($i = 0, 1$). We set U to be the guarded composition of U_0 and U_1 : $U = (|0\rangle \rightarrow U_0) \square (|1\rangle \rightarrow U_1)$. Then the super-operator defined by U is $\mathcal{E}(U) \in (|0\rangle \rightarrow \mathcal{E}_0) \square (|1\rangle \rightarrow \mathcal{E}_1)$. Indeed, we have:

$$(|0\rangle \rightarrow \mathcal{E}_0) \square (|1\rangle \rightarrow \mathcal{E}_1) = \{\mathcal{E}_\theta = U_\theta \circ U_\theta^\dagger : 0 \leq \theta < 2\pi\},$$

where $U_\theta = (|0\rangle \rightarrow U_0) \square (|1\rangle \rightarrow e^{i\theta} U_1)$. The non-uniqueness of the members of the above guarded composition is caused by the relative phase θ between U_0 and U_1 .

4 Semantics of QGCL

We first introduce several notations needed in this section. Let \mathcal{H} and \mathcal{H}' be two Hilbert spaces, and let E be an operator in \mathcal{H} . Then the cylindrical extension of E in $\mathcal{H} \otimes \mathcal{H}'$ is defined to be the operator $E \otimes I_{\mathcal{H}'}$, where $I_{\mathcal{H}'}$ is the identity operator in \mathcal{H}' . For simplicity, we will write E for $E \otimes I_{\mathcal{H}'}$ whenever confusion does not happen. Let F be an operator-valued function in \mathcal{H} over Σ . Then the cylindrical extension of F in $\mathcal{H} \otimes \mathcal{H}'$ is the operator-valued function F' in $\mathcal{H} \otimes \mathcal{H}'$ over Δ defined by $F'(\delta) = F(\delta) \otimes I_{\mathcal{H}'}$ for every $\delta \in \Delta$. For simplicity, we often write F for F' whenever confusion can be excluded from the context. Furthermore, let $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$ be a super-operator in \mathcal{H} . Then the cylindrical extension of \mathcal{E} in $\mathcal{H} \otimes \mathcal{H}'$ is defined to be the super-operator: $\mathcal{E} = \sum_i (E_i \otimes I_{\mathcal{H}'}) \circ (E_i^\dagger \otimes I_{\mathcal{H}'})$. Here, for simplicity, the same symbol \mathcal{E} is used to denote the extension of \mathcal{E} . In particular, if E is an operator in \mathcal{H} , and ρ is a partial density operator in $\mathcal{H} \otimes \mathcal{H}'$, then $E\rho E^\dagger$ should be understood as $(E \otimes I_{\mathcal{H}'})\rho(E^\dagger \otimes I_{\mathcal{H}'})$. If \mathcal{E}_1 and \mathcal{E}_2 are two super-operators in a Hilbert space \mathcal{H} , then their (sequential) composition $\mathcal{E}_1; \mathcal{E}_2$ is the super-operator in \mathcal{H} defined by $(\mathcal{E}_1; \mathcal{E}_2)(\rho) = \mathcal{E}_2(\mathcal{E}_1(\rho))$ for any partial density operator ρ in \mathcal{H} .

4.1 Classical states

We now define the states of classical variables in QGCL.

Definition 4.1 *The (partial) classical states and their domains are inductively defined as follows:*

1. ϵ is a classical state, called the empty state, and $\text{dom}(\epsilon) = \emptyset$;
2. If $x \in \text{Var}$ is a classical variable, and $a \in D_x$ is an element of the domain of x , then $[x \leftarrow a]$ is a classical state, and $\text{dom}([x \leftarrow a]) = \{x\}$;
3. If both δ_1 and δ_2 are classical states, and $\text{dom}(\delta_1) \cap \text{dom}(\delta_2) = \emptyset$, then $\delta_1\delta_2$ is a classical state, and $\text{dom}(\delta_1\delta_2) = \text{dom}(\delta_1) \cup \text{dom}(\delta_2)$;
4. If δ_i is a classical state for every $1 \leq i \leq n$, then $\oplus_{i=1}^n \delta_i$ is a classical state, and

$$\text{dom}(\oplus_{i=1}^n \delta_i) = \bigcup_{i=1}^n \text{dom}(\delta_i).$$

Intuitively, a classical state δ defined by clauses (1) to (3) in the above definition can be seen as a (partial) assignment to classical variables; more precisely, δ is an element of $\delta \in \prod_{x \in \text{dom}(\delta)} D_x$; that is, a choice function: $\delta : V \rightarrow \bigcup_{x \in \text{dom}(\delta)} D_x$ such that $\delta(x) \in D_x$ for every $x \in \text{dom}(\delta)$. In particular, ϵ is the empty function. Since $\prod_{x \in \emptyset} D_x = \{\epsilon\}$, ϵ is the only possible state of with empty domain. The state $[x \leftarrow a]$ assigns value a to variable x but the values of the other variables are undefined. The composed state $\delta_1\delta_2$ can be seen as the assignment to variables in $\text{dom}(\delta_1) \cup \text{dom}(\delta_2)$ given by

$$(\delta_1\delta_2)(x) = \begin{cases} \delta_1(x) & \text{if } x \in \text{dom}(\delta_1), \\ \delta_2(x) & \text{if } x \in \text{dom}(\delta_2). \end{cases} \quad (14)$$

Eq. (14) is well-defined since it is required that $\text{dom}(\delta_1) \cap \text{dom}(\delta_2) = \emptyset$. In particular, $\epsilon\delta = \delta\epsilon = \delta$ for any state δ , and if $x \notin \text{dom}(\delta)$ then $\delta[x \leftarrow a]$ is the assignment to variables in $\text{dom}(\delta) \cup \{x\}$ given by

$$\delta[x \leftarrow a](y) = \begin{cases} \delta(y) & \text{if } y \in \text{dom}(\delta), \\ a & \text{if } y = x. \end{cases}$$

The state $\oplus_{i=1}^n \delta_i$ defined by clause (4) in Definition 4.1 can be thought of as a kind of superposition of δ_i ($1 \leq i \leq n$).

4.2 Semi-classical denotational semantics

For each QGCL program P , we write $\Delta(P)$ for the set of all possible states of its classical variables. The semi-classical denotational semantics $\llbracket P \rrbracket$ of P will be defined as an operator-valued function in $\mathcal{H}_{\text{qvar}(P)}$ over $\Delta(P)$, where $\mathcal{H}_{\text{qvar}(P)}$ is the type of quantum variables occurring in P . In particular, if $\text{qvar}(P) = \emptyset$; for example $P = \text{abort}$ or skip , then $\mathcal{H}_{\text{qvar}(P)}$ is a one-dimensional space \mathcal{H}_\emptyset , and an operator in \mathcal{H}_\emptyset can be identified with a complex number; for instance the zero operator is number 0 and the identity operator is number 1. For any set $V \subseteq \text{qVar}$ of quantum variables, we write I_V for the identity operator in Hilbert space \mathcal{H}_V .

Definition 4.2 The classical state $\Delta(P)$ and semi-classical semantic function $\lceil P \rceil$ of a QGCL program P are inductively defined as follows:

1. $\Delta(\mathbf{abort}) = \{\epsilon\}$, and $\lceil \mathbf{abort} \rceil(\epsilon) = 0$;
2. $\Delta(\mathbf{skip}) = \{\epsilon\}$, and $\lceil \mathbf{skip} \rceil(\epsilon) = 1$;
3. $\Delta(U[\bar{q}]) = \{\epsilon\}$, and $\lceil U[\bar{q}] \rceil(\epsilon) = U_{\bar{q}}$, where $U_{\bar{q}}$ is the unitary operator U acting in $\mathcal{H}_{\bar{q}}$;

4. If $P \triangleq M[x \leftarrow \bar{q}] : \{P_m\}$, where $M = \{M_m\}$, then

$$\Delta(P) = \bigcup_m \{\delta[x \leftarrow m] : \delta \in \Delta(P_m)\},$$

$$\lceil P \rceil(\delta[x \leftarrow m]) = (\lceil P_m \rceil(\delta) \otimes I_{V \setminus \text{qvar}(P_m)}) \cdot (M_m \otimes I_{V \setminus \bar{q}})$$

for every $\delta \in \Delta(P_m)$ and for every m , where $V = \bar{q} \cup \bigcup_m \text{qvar}(P_m)$;

5. If $P \triangleq \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i$, then

$$\Delta(P) = \bigoplus_{i=1}^n \Delta(P_i),$$

$$\lceil P \rceil = \square_{i=1}^n |i\rangle \rightarrow \lceil P_i \rceil;$$

- 6.

$$\begin{aligned} \Delta(P_1; P_2) &= \Delta(P_1); \Delta(P_2) \\ &= \{\delta_1 \delta_2 : \delta_1 \in \Delta(P_1) \text{ and } \delta_2 \in \Delta(P_2)\}, \end{aligned} \tag{15}$$

$$\begin{aligned} \lceil P_1; P_2 \rceil(\delta_1 \delta_2) &= (\lceil P_2 \rceil(\delta_2) \otimes I_{V \setminus \text{qvar}(P_2)}) \\ &\quad \cdot (\lceil P_1 \rceil(\delta_1) \otimes I_{V \setminus \text{qvar}(P_1)}) \end{aligned}$$

where $V = \text{qvar}(P_1) \cup \text{qvar}(P_2)$;

Since it is required in Definition 2.1 that $\text{var}(P_1) \cap \text{var}(P_2) = \emptyset$ in the sequential composition $P_1; P_2$, we have $\text{dom}(\delta_1) \cap \text{dom}(\delta_2) = \emptyset$ for any $\delta_1 \in \Delta(P_1)$ and $\delta_2 \in \Delta(P_2)$. Thus, Eq. (15) is well-defined. Intuitively, if a quantum program P does not contain any guarded command, then its semantic structure can be seen as a tree with its nodes labelled by basic commands and its edges by linear operators. This tree grows up from the root in the following way: if the current node is labelled by a unitary transformation U , then a single edge stems from the node and it is labelled by U ; and if the current node is labelled by a measurement $M = \{M_m\}$, then for each possible outcome m , an edge stems from the node and it is labelled by the measurement operator M_m . Thus, each classical state $\delta \in \Delta(P)$ is corresponding to a branch in the semantic tree of P , and the value of semantic function $\lceil P \rceil$ in state δ is the (sequential) composition of the operators labelling the edges of δ . The semantic structure of a quantum program P with guarded commands is much more complicated. We can imagine it as a tree with superpositions of nodes that generate superpositions of branches. The value of semantic function $\lceil P \rceil$ in a superpositions of branches is then defined as the guarded composition of the values in these branches.

4.3 Purely quantum denotational semantics

Now the purely quantum semantics of a quantum program can be naturally defined as the super-operator induced by its semi-classical semantic function.

Definition 4.3 *For each QGCL program P , its purely quantum denotational semantics is the super-operator $\llbracket P \rrbracket$ in $\mathcal{H}_{qvar(P)}$ defined as follows:*

$$\llbracket P \rrbracket = \mathcal{E}(\lceil P \rceil) = \sum_{\delta \in \Delta(P)} \lceil P \rceil(\delta) \circ \lceil P \rceil(\delta)^\dagger.$$

The following proposition presents a representation of the purely quantum semantics of a program in terms of its subprograms.

Proposition 4.1 1. $\llbracket \text{abort} \rrbracket = 0$;

2. $\llbracket \text{skip} \rrbracket = 1$;

3. $\llbracket P_1; P_2 \rrbracket = \llbracket P_1 \rrbracket; \llbracket P_2 \rrbracket$;

4. $\llbracket U[\vec{q}] \rrbracket = U_{\vec{q}} \circ U_{\vec{q}}$;

5. $\llbracket M[x \leftarrow \vec{q}] : \{P_m\} \rrbracket = \sum_m \left[(M_m \circ M_m^\dagger); \llbracket P_m \rrbracket \right]$. Here, $\llbracket P_m \rrbracket$ should be seen as a cylindrical extension in \mathcal{H}_V from $\mathcal{H}_{qvar(P_m)}$, $M_m \circ M_m^\dagger$ as a cylindrical extension in \mathcal{H}_V from $\mathcal{H}_{\vec{q}}$, and $V = \vec{q} \cup \bigcup_m qvar(P_m)$;

6. $\llbracket \square_{i=1}^n \vec{q}, |i\rangle \rightarrow P_i \rrbracket \in \square_{i=1}^n |i\rangle \rightarrow \llbracket P_i \rrbracket$. Here $\llbracket P_i \rrbracket$ should be understood as a cylindrical extension in \mathcal{H}_V from $\mathcal{H}_{qvar(P_i)}$ for every $1 \leq i \leq n$, and $V = \vec{q} \cup \bigcup_{i=1}^n qvar(P_i)$.

The symbol “ \in ” in clause 6) of the above proposition can be understood as a refinement relation. It is worth noting that in general “ \in ” cannot be replaced by equality. This is exactly the reason that the purely quantum semantics of a program has to be derived through its semi-classical semantics and cannot be defined directly in a compositional way.

Equivalence relation between quantum programs can be introduced based on their purely quantum semantics.

Definition 4.4 *Let P and Q be two QGCL programs. If $qvar(P) = qvar(Q)$ and $\llbracket P \rrbracket = \llbracket Q \rrbracket$, then we say that P and Q are equivalent and write $P \equiv Q$.*

4.4 Weakest Precondition Semantics

The notion of quantum weakest precondition was proposed by D’Hondt and Panangaden [5].

Definition 4.5 *Let P be a program, and let M and N be positive (Hermitian) operators in $\mathcal{H}_{qvar(P)}$.*

1. If $\text{tr}(M\rho) \leq \text{tr}(N\llbracket P \rrbracket(\rho))$ for all $\rho \in \mathcal{D}(\mathcal{H}_{\text{qvar}(P)})$, then M is called a *precondition* of N with respect to P .
2. N is called the *weakest precondition* of M with respect to P , written $N = \text{wp}.P.M$ if
 - (a) N is a precondition of M with respect to P ; and
 - (b) $N' \sqsubseteq N$ whenever N' is also a precondition of M with respect to P .

$\text{wp}.P$ can be seen as the super-operator in $\mathcal{H}_{\text{qvar}(P)}$ defined as follows: for any positive operator M , $(\text{wp}.P)(M) = \text{wp}.P.M$ is given by clause 2) of the above definition, and $\text{wp}.P$ can be extended to the whole space $\mathcal{L}(\mathcal{H}_{\text{qvar}(P)})$ by linearity.

The weakest precondition semantics of QGCL programs are given in the next proposition.

Proposition 4.2 *For any QGCL program P , and for any positive (Hermitian) operator M in $\mathcal{H}_{\text{qvar}(P)}$, $\text{wp}.P.M$ is given as follows*

1. $\text{wp}.\mathbf{abort} = 0$;
2. $\text{wp}.\mathbf{skip} = 1$;
3. $\text{wp}.(P_1; P_2) = \text{wp}.P_2; \text{wp}.P_1$;
4. $\text{wp}.U[\bar{q}] = U_{\bar{q}}^\dagger \circ U_{\bar{q}}$;
5. $\text{wp}.(M[x \leftarrow \bar{q}] : \{P_m\}) = \sum_m \left[\text{wp}.P_m; (M_m^\dagger \circ M_m) \right]$;
6. $\text{wp}.(\square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i) \in \square_{i=1}^n |i\rangle \rightarrow \text{wp}.P_i$.

Some cylindrical extensions of super-operators are used but unspecified in the above proposition because they can be recognised from the context. Again, “ \in ” in the above clause 6) cannot be replaced by equality.

5 Quantum Choices: Superpositions of Programs

5.1 Definition and Example

As explained in Sec. 1, quantum choice may be defined based on quantum guarded command.

Definition 5.1 *Let P and P_i be programs for all $1 \leq i \leq n$ such that $\bar{q} = \text{qvar}(P)$. If $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}_{\bar{q}}$, and $\bar{q} \cap \bigcup_{i=1}^n \text{qVar}(P_i) = \emptyset$, then the quantum choice of P_1, \dots, P_n according to P along $\{|i\rangle\}$ is defined as*

$$\bigoplus_{i=1}^n P, |i\rangle \rightarrow P_i \triangleq P; \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i.$$

In particular, if $n = 2$, then the quantum choice will be abbreviated to $P_1 \text{ } P[\bar{q}] \oplus P_2$ or $P_1 \text{ } P \oplus P_2$.

Example 5.1 *Quantum walks have been extended to include multiple walkers and coins. These extended quantum walks can be conveniently written as QGCL programs with quantum choice. We consider two quantum walkers on a line sharing coins [16]. The Hilbert space of a single walker on a line is $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$, where $\mathcal{H}_p = \text{span}\{|x\rangle : x \in \mathbb{Z} \text{ (integers)}\}$ is the position space and $\mathcal{H}_c = \text{span}\{|L, R\rangle\}$ is the coin space. Its step operator is $W = (T_L \otimes |L\rangle\langle L| + T_R \otimes |R\rangle\langle R|)(I_{\mathcal{H}_p} \otimes H)$, where $I_{\mathcal{H}_p}$ is the identity operator in \mathcal{H}_p ,*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is the 2×2 Hadamard matrix, and T_L, T_R are left- and right-translation, respectively; that is, $T_L|x\rangle = |x-1\rangle$, $T_R|x\rangle = |x+1\rangle$ for every $x \in \mathbb{Z}$. Then the Hilbert space of two walkers is $\mathcal{H} \otimes \mathcal{H}$, and if the two walkers are independent, then the step operator is $W \otimes W$. A two-qubit unitary operator U can be introduced to entangle the two coins and it can be thought as that the two walkers are sharing coins. A step of two walkers sharing coins can be written as a QGCL program as follows:

$$U[c_1, c_2]; (T_L[q_1]_{H[c_1]} \oplus T_R[q_1]); (T_L[q_2]_{H[c_2]} \oplus T_R[q_2])$$

where q_1, q_2 are the position variables and c_1, c_2 the coin variables of the two walkers, respectively.

5.2 Local Quantum Variables

A quantum choice is defined as a “coin” program followed by a quantum guarded command. A natural question would be: is it possible to move the “coin” program to the end of a guarded command? To answer this question positively, we need to extend the syntax of QGCL by introducing block command with local quantum variables.

Definition 5.2 *Let P be a QGCL program, let $\bar{q} \subseteq \text{qvar}(P)$ be a sequence of quantum variables, and let ρ be a density operator in $\mathcal{H}_{\bar{q}}$. Then*

1. *The block command defined by P restricted to $\bar{q} = \rho$ is:*

$$\mathbf{begin\ local\ } \bar{q} := \rho; P \mathbf{end}.$$

2. *The quantum variables of the block command are:*

$$\text{qvar}(\mathbf{begin\ local\ } \bar{q} := \rho; P \mathbf{end}) = \text{qvar}(P) \setminus \bar{q}.$$

3. *The purely quantum denotational semantics of the block command is give as follows:*

$$\llbracket \mathbf{begin\ local\ } \bar{q} := \rho; P \mathbf{end} \rrbracket (\sigma) = \text{tr}_{\mathcal{H}_{\bar{q}}}(\llbracket P \rrbracket (\sigma \otimes \rho))$$

for any density operator σ in $\mathcal{H}_{\text{qvar}(P) \setminus \bar{q}}$.

The following theorem shows that the “coin” in a quantum choice can be move to the end of the guarded command if encapsulation in a block with local variables is allowed.

Theorem 5.1

$$\bigoplus_{i=1}^n U[\bar{q}], |i\rangle \rightarrow P_i \equiv (\Box_{i=1}^n U_{\bar{q}}^\dagger |i\rangle \rightarrow P_i); U[\bar{q}]. \quad (16)$$

More generally, we have:

$$\begin{aligned} \bigoplus_{i=1}^n P, |i\rangle \rightarrow P_i &\equiv \mathbf{begin\ local\ } \bar{r} := |\varphi_0\rangle; \\ &\quad \Box_{i,j} |\psi_{ij}\rangle \rightarrow Q_{ij}; U[\bar{q}, \bar{r}] \mathbf{end} \end{aligned} \quad (17)$$

for some new quantum variables \bar{r} , state $|\varphi_0\rangle \in \mathcal{H}_{\bar{r}}$, orthonormal basis $\{|\psi_{ij}\rangle\}$ of $\mathcal{H}_{\bar{q}} \otimes \mathcal{H}_{\bar{r}}$, programs Q_{ij} , and unitary operator U in $\mathcal{H}_{\bar{q}} \otimes \mathcal{H}_{\bar{r}}$, where $\bar{q} = \text{qvar}(P)$.

5.3 Quantum implementation of probabilistic choices

We now examine the relation between probabilistic choice and quantum choice. To this end, we first extend the syntax of QGCL by adding probabilistic choice.

Definition 5.3 Let P_i be a QGCL program for each $1 \leq i \leq n$, and let $\{p_i\}_{i=1}^n$ be a sub-probability distribution; that is, $p_i \geq 0$ for each $1 \leq i \leq n$ and $\sum_{i=1}^n p_i \leq 1$. Then

1. The probabilistic choice of P_1, \dots, P_n according to $\{p_i\}_{i=1}^n$ is

$$\sum_{i=1}^n P_i @ p_i.$$

2. The quantum variables of the choice are:

$$\text{qvar} \left(\sum_{i=1}^n P_i @ p_i \right) = \bigcup_{i=1}^n \text{qvar}(P_i).$$

3. The purely quantum denotational semantics of the choice is:

$$\left[\sum_{i=1}^n P_i @ p_i \right] = \sum_{i=1}^n p_i \cdot \llbracket P_i \rrbracket.$$

Example 5.2 (Continuation of Example 3.3; Probabilistic mixture of measurements) It is often required in quantum cryptographic protocols like BB84 to randomly choose between the measurement M^0 on a qubit in the computational basis and the measurement M^1 in the basis $|\pm\rangle$. If we perform measurement M^i on qubit $|\psi\rangle$ and discard the outcomes

of measurement, then we get $\rho_i = M_0^i |\psi\rangle\langle\psi| M_0^i + M_1^i |\psi\rangle\langle\psi| M_1^i$ for $i = 0, 1$. We now consider the unitary matrix

$$U = \begin{pmatrix} \sqrt{p} & \sqrt{q} \\ \sqrt{q} & -\sqrt{p} \end{pmatrix}$$

on a qubit, where $p, q \geq 0$ and $p + q = 1$. Let

$$P \triangleq \textbf{begin local } q := |0\rangle; q := U[q]; \\ \square_{i=0,1} q, |i\rangle \rightarrow M_i[q_1] \textbf{end}$$

where q, q_1 are qubit variables. Then for any $|\psi\rangle \in \mathcal{H}_{q_1}$ and $i, j \in \{0, 1\}$, we have:

$$\begin{aligned} |\psi_{ij}\rangle &\triangleq M_{ij}(|\psi\rangle U|0\rangle) = \sqrt{\frac{p}{2}} M_i^0 |\psi\rangle |0\rangle + \sqrt{\frac{q}{2}} M_j^1 |\psi\rangle |1\rangle, \\ \llbracket P \rrbracket(|\psi\rangle\langle\psi|) &= \text{tr}_{\mathcal{H}_q} \left(\sum_{i,j=0,1} |\psi_{ij}\rangle\langle\psi_{ij}| \right) \\ &= \sum_{i,j=0,1} \left(\frac{p}{2} M_i^0 |\psi\rangle\langle\psi| M_i^0 + \frac{q}{2} M_j^1 |\psi\rangle\langle\psi| M_j^1 \right) \\ &= p\rho_0 + q\rho_1. \end{aligned}$$

So, program P can be seen as a probabilistic mixture of measurements M^0 and M^1 .

As shown by the following theorem, if the “coin” variables are treated as local variables, then a quantum choice degenerates to a probabilistic choice.

Theorem 5.2 *Let $\text{qvar}(P) = \bar{q}$. Then we have:*

$$\textbf{begin local } \bar{q} := \rho; \bigoplus_{i=1}^n P, |i\rangle \rightarrow P_i \textbf{end} \equiv \sum_{i=1}^n P_i @ p_i$$

where $p_i = \langle i | \llbracket P \rrbracket(\rho) | i \rangle$ for every $1 \leq i \leq n$.

Conversely, for any probability distribution $\{p_i\}_{i=1}^n$, we can find an $n \times n$ unitary operator U such that $p_i = |U_{i0}|^2$ ($1 \leq i \leq n$). So, it follows immediately from the above theorem that a probabilistic choice $\sum_{i=1}^n P_i @ p_i$ can always be implemented by a quantum choice:

$$\textbf{begin local } \bar{q} := |0\rangle; \bigoplus_{i=1}^n U[\bar{q}], |i\rangle \rightarrow P_i \textbf{end}$$

where \bar{q} is a family of new quantum variables with an n -dimensional state space.

6 Quantum Recursion

Now we need to further extend the syntax of QGCL. We first add a countable set of program names, ranged over by X, Y, \dots , to the alphabet of QGCL, and then introduce the following:

Definition 6.1 *QGCL programs are defined by combining Definitions 2.1, 5.2, 5.3 and the following two clauses:*

1. Every program name X is a program, and both $\text{var}(X)$ and $\text{qvar}(X)$ are given a priori.
2. If P is a program and X a program name such that $\text{var}(P) \subseteq \text{var}(X)$ and $\text{qvar}(P) \subseteq \text{qvar}(X)$, then $\mu X.P$ is a program, and $\text{var}(\mu X.P) = \text{var}(X)$, $\text{qvar}(\mu X.P) = \text{qvar}(X)$.

We consider a special case of quantum recursion, namely quantum loop, and show an interesting difference between quantum loops with classical control flows defined in [18] and quantum loops with quantum control flows. The quantum loops considered in [18] can be written as QGCL programs of the form:

$$\begin{aligned} \text{Loop} &= \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ \bar{q} := U\bar{q} \\ &\triangleq \mu X.M[x \leftarrow \bar{q}] : \{P_0 = \mathbf{skip}, P_1 = \bar{q} := U\bar{q}; X\} \end{aligned}$$

where \bar{q} is a sequence of quantum variables, $M = \{M_0, M_1\}$ a binary (“yes-no”) measurement in $\mathcal{H}_{\bar{q}}$ and U a unitary operator in $\mathcal{H}_{\bar{q}}$. The control flow of Loop is determined by measurement M in the loop guard: if the outcome of measurement is 0 then P_0 is executed - the loop terminates; if the outcome of measurement is 1 then P_1 is executed - the program executes the loop body $\bar{q} := U\bar{q}$ and then runs into the loop again. Program Loop can be approximated by a series of iterations $\{Q_n\}_{n=0}^\infty$ defined as follows:

$$\begin{cases} Q_0 & \triangleq \mathbf{abort}, \\ Q_{n+1} & \triangleq M[x \leftarrow \bar{q}] : \{P_0 = \mathbf{skip}, \\ & P_1^{(n+1)} = \bar{q} := U\bar{q}; Q_n\} \ (n \geq 0). \end{cases} \quad (18)$$

If the classical control flows of Q_n ($n \geq 0$) determined by the outcomes of measurement M are replaced by quantum control flows defined by quantum choices, then we obtain the following quantum iterations:

$$\begin{cases} Q'_0 & \triangleq \mathbf{abort}, \\ Q'_{n+1} & \triangleq \mathbf{skip}_{C[q_{n+1}]} \oplus (\bar{q} := U\bar{q}; Q'_n) \ (n \geq 0) \end{cases}$$

where C is a “coin” 2×2 unitary matrix. It is worth noting that we have to introduce a sequence q_1, q_2, \dots of new qubit variables in order to well-define the quantum choices used

in Q'_n ($n \geq 1$). For each $n \geq 0$, since $\text{var}(Q'_n) = \emptyset$ and $\text{qvar}(Q'_n) = \bar{q} \cup \{q_1, \dots, q_n\}$, the semi-classical semantics $\llbracket Q'_n \rrbracket$ of Q'_n is an operator-valued function in $\mathcal{H}_{\bar{q}} \otimes \bigotimes_{i=1}^n \mathcal{H}_{q_i}$ over $\{\epsilon\}$. Suppose that the input is a state $|\psi\rangle$ in $\mathcal{H}_{\bar{q}}$, and all the auxiliary qubit variables q_1, \dots, q_n are initialised in state $|0\rangle$. For simplicity of calculation, we take $C = H$ (the 2×2 Hadamard matrix; see Example 5.1). Then

$$\llbracket Q'_n \rrbracket(\epsilon)|\psi\rangle|0\rangle^n = \sum_{i=0}^{n-1} \frac{1}{\sqrt{2^{i+1}}} U^i |\psi\rangle|0\rangle^{n-i}|1\rangle^i.$$

It is clear that we cannot directly define the semantics of a quantum loop as the limit of $\{Q'_n\}_{n=0}^\infty$ because the state spaces of Q'_n are different for different n . To overcome this difficulty, a natural idea is to localise qubit variables q_1, \dots, q_n :

$$Q''_n = \text{begin local } q_1, \dots, q_n := |0\rangle^n; Q'_n \text{ end}.$$

But such a localisation makes the quantum iterations degenerate to probabilistic iterations:

$$\llbracket Q''_n \rrbracket(\rho) = \sum_{i=0}^{n-1} \frac{1}{2^{i+1}} U^i \rho (U^\dagger)^i.$$

This gives an example showing that quantum loops, or more generally quantum recursions, with quantum control flows are much harder to deal with than those with classical control flows. Due to the limited space, a more detailed treatment of quantum recursion is postponed to another paper.

7 Conclusions

Three new quantum program constructs - quantum guarded command, quantum choice and quantum recursion - are defined in this paper. We believe that introducing these constructs is a significant step toward the full realisation of “quantum control” in quantum programming. In the further studies, we will consider quantum recursions with quantum controls in detail, and we will establish various algebraic laws for QGCL programs that can be used in program transformations and compilation. A quantum Floyd-Hoare logic was built in [17] for quantum programs with only classical control flows. So, another interesting topic for further studies would be to extend this logic so that it can also be applied to programs with quantum control flows.

References

- [1] D. Aharonov, A. Ambainis, J. Kempe and U. Vazirani, Quantum walks on graphs, *Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC)*, 2001, pp. 50-59.

- [2] T. Altenkirch and J. Grattage, A functional quantum programming language, *Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science (LICS)*, 2005, pp. 249-258.
- [3] T. Altenkirch, J. Grattage, J. K. Vizzotto and A. Sabry, An algebra of pure quantum programming, *Electronic Notes in Theoretical Computer Science*, 170(2007)23-47.
- [4] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath and J. Watrous, One-dimensional quantum walks, *Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC)*, 2001, pp. 37-49.
- [5] E. D'Hondt and P. Panangaden, Quantum weakest preconditions, *Mathematical Structures in Computer Science*, 16(2006)429-451.
- [6] E. W. Dijkstra, Guarded commands, nondeterminacy and formal derivation of programs, *Communications of the ACM*, 18(1975)453-457.
- [7] S. Gay, Quantum programming languages: survey and bibliography, *Mathematical Structures in Computer Science*, 16(2006)581-600.
- [8] E. H. Knill, *Conventions for quantum pseudocode*, Technical Report LAUR-96-2724, Los Alamos National Laboratory, 1996.
- [9] M. Lampis, K. G. Ginis, M. A. Papakyriakou and N. S. Papaspyrou, Quantum data and control made easier, *Electronic Notes in Theoretical Computer Science*, 210(2008)85-105.
- [10] A. McIver and C. Morgan, *Abstraction, Refinement and Proof for Probabilistic Systems*, Springer, New York, 2005.
- [11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (2000)
- [12] B. Ömer, *Structural quantum programming*, Ph.D. Thesis, Technical University of Vienna, 2003.
- [13] J. W. Sanders and P. Zuliani, Quantum programming, *Proceedings of Mathematics of Program Construction 2000*, LNCS 1837, Springer-Verlag, pp. 88-99.
- [14] P. Selinger, Towards a quantum programming language, *Mathematical Structures in Computer Science*, 14(2004)527-586.
- [15] V. V. Shende, S. S. Bullock and I. L. Markov, Synthesis of quantum-logic circuits, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25(2006)1000-1010.
- [16] P. Xue and B. C. Sanders, Two quantum walkers sharing coins, *Physical Review A*, 85(2012) art. no. 022307.

- [17] M. S. Ying, Floyd-Hoare logic for quantum programs, *ACM Transactions on Programming Languages and Systems*, 39(2011) art. no. 19.
- [18] M. S. Ying and Y. Feng, Quantum loop programs, *Acta Informatica*, 47(2010)221-250.

Appendix: Proofs

7.1 Proof of Lemma 3.2

We start with an auxiliary equality. Put:

$$\overline{F} \triangleq \sum_{\delta_1 \in \Delta_1, \dots, \delta_n \in \Delta_n} F(\oplus_{i=1}^n \delta_i)^\dagger \cdot F(\oplus_{i=1}^n \delta_i).$$

For any $|\varphi\rangle, |\psi\rangle \in \mathcal{H} \otimes \mathcal{H}_s$, we can write:

$$\begin{aligned} |\varphi\rangle &= \sum_{i=1}^n |\varphi_i\rangle |i\rangle, \\ |\psi\rangle &= \sum_{i=1}^n |\psi_i\rangle |i\rangle \end{aligned}$$

where $|\varphi_i\rangle, |\psi_i\rangle \in \mathcal{H}$ for each $1 \leq i \leq n$. Then

$$\begin{aligned} \langle \varphi | \overline{F} | \psi \rangle &= \sum_{\delta_1, \dots, \delta_n} \langle \varphi | F(\oplus_{i=1}^n \delta_i)^\dagger \cdot F(\oplus_{i=1}^n \delta_i) | \psi \rangle \\ &= \sum_{\delta_1, \dots, \delta_n} \sum_{i, i'=1}^n \left(\prod_{k \neq i} \lambda_{k\delta_k}^* \right) \left(\prod_{k \neq i'} \lambda_{k\delta_k} \right) \\ &\quad \langle \varphi_i | F_i(\delta_i)^\dagger F_{i'}(\delta_{i'}) | \psi_{i'} \rangle \langle i | i' \rangle \\ &= \sum_{\delta_1, \dots, \delta_n} \sum_{i=1}^n \left(\prod_{k \neq i} |\lambda_{k\delta_k}|^2 \right) \langle \varphi_i | F_i(\delta_i)^\dagger F_i(\delta_i) | \psi_i \rangle \\ &= \sum_{i=1}^n \sum_{\delta_1, \dots, \delta_{i-1}, \delta_{i+1}, \dots, \delta_n} \left(\prod_{k \neq i} |\lambda_{k\delta_k}|^2 \right) \\ &\quad \sum_{\delta_i} \langle \varphi_i | F_i(\delta_i)^\dagger F_i(\delta_i) | \psi_i \rangle \\ &= \sum_{i=1}^n \sum_{\delta_i} \langle \varphi_i | F_i(\delta_i)^\dagger F_i(\delta_i) | \psi_i \rangle \\ &= \sum_{i=1}^n \langle \varphi_i | \sum_{\delta_i} F_i(\delta_i)^\dagger F_i(\delta_i) | \psi_i \rangle \end{aligned} \tag{19}$$

because for each k , we have:

$$\sum_{\delta_k} |\lambda_{k\delta_k}|^2 = 1,$$

and thus

$$\sum_{\delta_1, \dots, \delta_{i-1}, \delta_{i+1}, \dots, \delta_n} \left(\prod_{k \neq i} |\lambda_{k\delta_k}|^2 \right) = \prod_{k \neq i} \left(\sum_{\delta_k} |\lambda_{k\delta_k}|^2 \right) = 1. \tag{20}$$

(1) We now prove that F is a semi-classical semantic function in $\mathcal{H} \otimes \mathcal{H}_s$ over $\bigoplus_{i=1}^n \Delta_n$. It suffices to show that $\overline{F} \sqsubseteq I_{\mathcal{H} \otimes \mathcal{H}_s}$; that is, $\langle \varphi | \overline{F} | \varphi \rangle \leq \langle \varphi | \varphi \rangle$ for each $|\varphi\rangle \in \mathcal{H} \otimes \mathcal{H}_s$. In fact, for each $1 \leq i \leq n$, since F_i is a semi-classical semantic function, we have:

$$\sum_{\delta_i} F_i(\delta_i)^\dagger F_i(\delta_i) \sqsubseteq I_{\mathcal{H}},$$

$$\langle \varphi_i | \sum_{\delta_i} F_i(\delta_i)^\dagger F_i(\delta_i) | \varphi_i \rangle \leq \langle \varphi_i | \varphi_i \rangle.$$

Then it follows from Eq. (19) that

$$\langle \varphi | \overline{F} | \varphi \rangle \leq \sum_{i=1}^n \langle \varphi_i | \varphi_i \rangle = \langle \varphi | \varphi \rangle.$$

(2) For the case where all F_i ($1 \leq i \leq n$) are full, we have:

$$\sum_{\delta_i} F_i(\delta_i)^\dagger F_i(\delta_i) = I_{\mathcal{H}}$$

for all $1 \leq i \leq n$, and it follows from Eq. (19) that

$$\langle \varphi | \overline{F} | \psi \rangle = \sum_{i=1}^n \langle \varphi_i | \psi_i \rangle = \langle \varphi | \psi \rangle.$$

So, it holds that $\overline{F} = I_{\mathcal{H} \otimes \mathcal{H}_s}$ by arbitrariness of $|\varphi\rangle$ and $|\psi\rangle$, and F is full.

7.2 Proof of Proposition 4.1

Clauses 1) - 4) are obvious.

5) By definition, for any partial density operator ρ in $\mathcal{H}_{qvar(P)}$, we have:

$$\begin{aligned} & \llbracket M[x\vec{q}] : \{P_m\} \rrbracket(\rho) \\ &= \sum_m \sum_{\delta \in \Delta(P_m)} \lceil P \rceil(\delta[x \leftarrow m]) \rho \lceil P \rceil(\delta[x \leftarrow m])^\dagger \\ &= \sum_m \sum_{\delta \in \Delta(P_m)} (\lceil P_m \rceil(\delta) \otimes I_{qvar(P) \setminus qvar(P_m)}) \\ & \quad (M_m \otimes I_{qvar(P) \setminus \vec{q}}) \rho (M_m^\dagger \otimes I_{qvar(P) \setminus \vec{q}}) \\ & \quad (\lceil P_m \rceil(\delta)^\dagger \otimes I_{V \setminus qvar(P_m)}) \\ &= \sum_m \sum_{\delta \in \Delta(P_m)} (\lceil P_m \rceil(\delta) \otimes I_{qvar(P) \setminus qvar(P_m)}) \\ & \quad (M_m \rho M_m^\dagger) (\lceil P_m \rceil(\delta)^\dagger \otimes I_{V \setminus qvar(P_m)}) \\ &= \sum_m \llbracket P_m \rrbracket (M_m \rho M_m^\dagger) \\ &= \left(\sum_m (M_m \circ M_m^\dagger); \llbracket P_m \rrbracket \right) (\rho). \end{aligned}$$

6) For simplicity of the presentation, we write:

$$P \triangleq \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i.$$

By definition, we obtain:

$$\llbracket P \rrbracket = \mathcal{E}(\lceil \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i \rceil).$$

Since

$$\lceil \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i \rceil = \square_{i=1}^n \bar{q}, |i\rangle \rightarrow \lceil P_i \rceil$$

and $\lceil P_i \rceil \in \mathbb{F}(\llbracket P_i \rrbracket)$ for every $1 \leq i \leq n$, it holds that

$$\begin{aligned} \llbracket P \rrbracket &\in \{ \mathcal{E}(\square_{i=1}^n |i\rangle \rightarrow F_i) : F_i \in \mathbb{F}(\llbracket P_i \rrbracket) \\ &\text{for every } 1 \leq i \leq n \} = \square_{i=1}^n |i\rangle \rightarrow \llbracket P_i \rrbracket. \end{aligned}$$

7.3 Proof of Proposition 4.2

The proof is based on the following key lemma by D'Hondt and Panangaden [5].

Lemma 7.1 *If the semantic function $\llbracket P \rrbracket$ of program P has the Kraus operator-sum representation: $\llbracket P \rrbracket = \sum_j E_j \circ E_j^\dagger$, then we have: $wp.P = \sum_j E_j^\dagger \circ E_j$.*

Now we start to prove Proposition 4.2. Clauses 1) - 4) are immediate from Proposition 4.1 and Lemma 7.1.

5) Suppose that for every m ,

$$\llbracket P_m \rrbracket = \sum_m E_{mi_m} \circ E_{mi_m}^\dagger.$$

Then by Proposition 4.1 5) we have:

$$\begin{aligned} \llbracket M[x \leftarrow \bar{q}] : \{P_m\} \rrbracket &= \sum_m \left[(M_m \circ M_m^\dagger); \llbracket P_m \rrbracket \right] \\ &= \sum_m \left[(M_m \circ M_m^\dagger); \sum_{i_m} (E_{mi_m} \circ E_{mi_m}^\dagger) \right] \\ &= \sum_m \sum_{i_m} (E_{mi_m} M_m) \circ (M_m^\dagger E_{mi_m}^\dagger) \\ &= \sum_m \sum_{i_m} (E_{mi_m} M_m) \circ (E_{mi_m} M_m)^\dagger. \end{aligned}$$

Using Lemma 7.1 we obtain:

$$\begin{aligned}
wp.(M[x \leftarrow \bar{q}]; \{P_m\}) &= \sum_m \sum_{i_m} (E_{mi_m} M_m)^\dagger \circ (E_{mi_m} M_m) \\
&= \sum_m \sum_{i_m} \left(M_m^\dagger E_{mi_m}^\dagger \right) \circ (E_{mi_m} M_m) \\
&= \sum_m \left[\sum_{i_m} \left(E_{mi_m}^\dagger \circ E_{mi_m} \right); \left(M_m^\dagger \circ M_m \right) \right] \\
&= \sum_m \left[wp.P_m; (M_m^\dagger \circ M_m) \right].
\end{aligned}$$

6) For each $1 \leq i \leq n$, assume that the semi-classical semantics of P_i is the function $\llbracket P_i \rrbracket$ over $\Delta = \{j_i\}$ such that

$$\llbracket P_i \rrbracket(j_i) = E_{ij_i}$$

for every j_i . Then by Definition 4.3 we obtain:

$$\llbracket P_i \rrbracket = \sum_{j_i} E_{ij_i} \circ E_{ij_i}^\dagger,$$

and it follows from Lemma 7.1 that

$$wp.P_i = \sum_{j_i} E_{ij_i}^\dagger \circ E_{ij_i}.$$

For any $|\varphi\rangle = \sum_{i=1}^n |\varphi_i\rangle |i\rangle$, where $|\varphi_i\rangle \in \mathcal{H}_{qvar(P_i)}$ ($1 \leq i \leq n$), we define:

$$\begin{aligned}
G_{j_1 \dots j_n}(|\varphi\rangle) &= \sum_{i=1}^n \zeta_i E_{ij_i}^\dagger |\varphi_i\rangle |i\rangle, \\
\zeta_i &= \prod_{k \neq i} \delta_{kj_k},
\end{aligned}$$

$$\delta_{kj_k} = \sqrt{\frac{tr(E_{kj_k}^\dagger)^\dagger E_{kj_k}^\dagger}{\sum_{l_k} (E_{kl_k}^\dagger)^\dagger E_{kl_k}^\dagger}} = \sqrt{\frac{tr E_{kj_k}^\dagger E_{kj_k}}{\sum_{l_k} E_{kl_k}^\dagger E_{kl_k}}} = \lambda_{kj_k} \quad (21)$$

and λ_{kj_k} 's are defined by Eq. (13). By Definitions 3.4 and 3.5 we have:

$$\sum_{j_1, \dots, j_n} G_{j_1 \dots j_n} \circ G_{j_1 \dots j_n}^\dagger \in \square_{i=1}^n |i\rangle \rightarrow wp.P_i.$$

On the other hand, by Definitions 4.2 (5) and 4.3 we have:

$$\llbracket \square_{i=1}^n q, |i\rangle \rightarrow P_i \rrbracket = \sum_{j_1, \dots, j_n} F_{j_1 \dots j_n} \circ F_{j_1 \dots j_n}^\dagger$$

where $F_{j_1 \dots j_n}$'s are defined by Eq. (12). Applying Lemma 7.1 once again, we obtain:

$$wp.(\square_{i=1}^n q, |i\rangle \rightarrow P_i) = \sum_{j_1, \dots, j_n} F_{j_1 \dots j_n}^\dagger \circ F_{j_1 \dots j_n}.$$

So, we now only need to prove that

$$G_{j_1 \dots j_n} = F_{j_1 \dots j_n}^\dagger$$

for all j_1, \dots, j_n . In fact, for any $|\psi\rangle = \sum_{i=1}^n |\psi_i\rangle |i\rangle$ with $|\psi_i\rangle \in \mathcal{H}_{\text{var}(P_i)}$ ($1 \leq i \leq n$), it holds that

$$\begin{aligned} (G_{j_1 \dots j_n} |\varphi\rangle, |\psi\rangle) &= \left(\sum_{i=1}^n \zeta_i E_{ij_i}^\dagger |\varphi_i\rangle |i\rangle, \sum_{i=1}^n |\psi_i\rangle |i\rangle \right) \\ &= \sum_{i, i'} \zeta_i^* (E_{ij_i}^\dagger |\varphi_i\rangle, |\psi_{i'}\rangle) \langle i | i' \rangle \\ &= \sum_i \zeta_i (E_{ij_i}^\dagger |\varphi_i\rangle, |\psi_i\rangle) \\ &= \sum_i \zeta_i (|\varphi_i\rangle, E_{ij_i} |\psi_i\rangle) \\ &= \sum_{i, i'} \zeta_i (|\varphi_i\rangle, E_{i'j_{i'}} |\psi_{i'}\rangle) \langle i | i' \rangle \\ &= \left(\sum_{i=1}^n |\varphi_i\rangle |i\rangle, \sum_{i=1}^n \zeta_i E_{ij_i} |\psi_i\rangle |i\rangle \right) \\ &= (|\varphi\rangle, F_{j_1 \dots j_n} |\psi\rangle) \end{aligned}$$

because ζ_i 's are real numbers, and it follows from Eq. (21) that

$$\zeta_i = \prod_{k \neq i} \lambda_{kj_k}$$

for each $1 \leq i \leq n$. Thus, we complete the proof.

7.4 Proof of Theorem 5.1

We first prove Eq. (16). Assume that $[P_i]$ is the operator-valued function over Δ_i such that $[P_i](\delta_i) = F_{i\delta_i}$ for each $\delta_i \in \Delta_i$ ($1 \leq i \leq n$). We write:

$$P = \square_{i=1}^n U_q^\dagger |i\rangle \rightarrow P_i.$$

Then for any $|\psi\rangle = \sum_{i=1}^n |\psi_i\rangle|i\rangle$, where $|\psi_i\rangle \in \mathcal{H}_V$ ($1 \leq i \leq n$), and $V = \bigcup_{i=1}^n \text{qvar}(P_i)$, we have:

$$\begin{aligned}
& [P](\oplus_{i=1}^n \delta_i)|\psi\rangle \\
&= [P](\oplus_{i=1}^n \delta_i) \left[\sum_{i=1}^n |\psi_i\rangle \left(\sum_{j=1}^n U_{ij}(U_{\bar{q}}^\dagger|j\rangle) \right) \right] \\
&= [P](\oplus_{i=1}^n \delta_i) \left[\sum_{j=1}^n \left(\sum_{i=1}^n U_{ij}|\psi_i\rangle \right) (U_{\bar{q}}^\dagger|j\rangle) \right] \\
&= \sum_{j=1}^n \left(\prod_{k \neq j} \lambda_k \delta_k \right) F_{j\delta_j} \left(\sum_{i=1}^n U_{ij}|\psi_i\rangle \right) (U_{\bar{q}}^\dagger|j\rangle).
\end{aligned}$$

Let LHS and RHS stand for the left and right hand side of Eq. (16), respectively. Then it holds that

$$\begin{aligned}
& [RHS](\oplus_{i=1}^n \delta_i)|\psi\rangle = U_{\bar{q}}([P](\oplus_{i=1}^n \delta_i)|\psi\rangle) \\
&= \sum_{j=1}^n \left(\prod_{k \neq j} \lambda_k \delta_k \right) F_{j\delta_j} \left(\sum_{i=1}^n U_{ij}|\psi_i\rangle \right) |j\rangle \\
&= [\square_{i=1}^n |i\rangle \rightarrow P_i](\oplus_{i=1}^n \delta_i) \left[\sum_{j=1}^n \left(\sum_{i=1}^n U_{ij}|\psi_i\rangle \right) |j\rangle \right] \\
&= [\square_{i=1}^n |i\rangle \rightarrow P_i](\oplus_{i=1}^n \delta_i) \left[\sum_{i=1}^n |\psi_i\rangle \sum_{j=1}^n (U_{ij}|j\rangle) \right] \\
&= [\square_{i=1}^n |i\rangle \rightarrow P_i](\oplus_{i=1}^n \delta_i) \left(\sum_{i=1}^n |\psi_i\rangle (U_{\bar{q}}|i\rangle) \right) \\
&= [LHS](\oplus_{i=1}^n \delta_i)|\psi\rangle.
\end{aligned}$$

Consequently, it follows that $\llbracket LHS \rrbracket = \llbracket RHS \rrbracket$ and we complete the proof of Eq. (16).

Now we are ready to prove Eq. (17). Since $\llbracket P \rrbracket$ is a super-operator in $\mathcal{H}_{\bar{q}}$, there must be a family of quantum variables \bar{r} , a pure state $|\varphi_0\rangle \in \mathcal{H}_{\bar{r}}$, a unitary operator U in $\mathcal{H}_{\bar{q}} \otimes \mathcal{H}_{\bar{r}}$, and a projection operator K onto some closed subspace \mathcal{K} of $\mathcal{H}_{\bar{r}}$ such that

$$\llbracket P \rrbracket(\rho) = \text{tr}_{\mathcal{H}_{\bar{r}}}(KU(\rho \otimes |\varphi_0\rangle\langle\varphi_0|)U^\dagger K)$$

for all density operators ρ in $\mathcal{H}_{\bar{q}}$ (see the system-environment model of super-operators, Eq. (8.38) in [11]). We choose an orthonormal basis of \mathcal{K} and then extend it to an orthonormal basis $\{|j\rangle\}$ of $\mathcal{H}_{\bar{r}}$. Define pure states $|\psi_{ij}\rangle = U^\dagger|i\rangle|j\rangle$ for all i, j and programs

$$Q_{ij} = \begin{cases} P_i & \text{if } |j\rangle \in \mathcal{K}, \\ \text{abort} & \text{if } |j\rangle \notin \mathcal{K}. \end{cases}$$

Then by a routine calculation we have:

$$\llbracket \square_{i,j} |ij\rangle \rightarrow Q_{ij} \rrbracket(\sigma) = \llbracket \square_i |i\rangle \rightarrow P_i \rrbracket(K\sigma K) \quad (22)$$

for any $\sigma \in \mathcal{H}_{\bar{q} \cup \bar{r} \cup V}$, where $V = \bigcup_{i=1}^n \text{qvar}(P_i)$. We now write *RHS* for the right hand side of Eq. (17). Combining Eqs (16) and (22), we obtain:

$$\begin{aligned} & \llbracket RHS \rrbracket(\rho) \\ &= \text{tr}_{\mathcal{H}_{\bar{r}}} \left(\llbracket \square_{i,j} U^\dagger |ij\rangle \rightarrow Q_{ij}; U[\bar{q}, \bar{r}] \rrbracket(\rho \otimes |\varphi_0\rangle\langle\varphi_0|) \right) \\ &= \text{tr}_{\mathcal{H}_{\bar{r}}} \left(\llbracket \bigoplus_{i,j} U^\dagger U[\bar{q}, \bar{r}], |ij\rangle \rightarrow Q_{ij} \rrbracket(\rho \otimes |\varphi_0\rangle\langle\varphi_0|) \right) \\ &= \text{tr}_{\mathcal{H}_{\bar{r}}} \left(\llbracket \square_{i,j} |ij\rangle \rightarrow Q_{ij} \rrbracket(U(\rho \otimes |\varphi_0\rangle\langle\varphi_0|)U^\dagger) \right) \\ &= \text{tr}_{\mathcal{H}_{\bar{r}}} \llbracket \square_i |i\rangle \rightarrow P_i \rrbracket(KU(\rho \otimes |\varphi_0\rangle\langle\varphi_0|)U^\dagger K) \\ &= \llbracket \square_i |i\rangle \rightarrow P_i \rrbracket(\text{tr}_{\mathcal{H}_{\bar{r}}}(KU(\rho \otimes |\varphi_0\rangle\langle\varphi_0|)U^\dagger K)) \\ &= \llbracket \square_i |i\rangle \rightarrow P_i \rrbracket(\llbracket P \rrbracket(\rho)) \\ &= \llbracket \bigoplus_i P, |i\rangle \rightarrow P_i \rrbracket(\rho) \end{aligned}$$

for all density operators ρ in $\mathcal{H}_{\bar{q}}$. Therefore, Eq. (17) is proved.

7.5 Proof of Theorem 5.2

To simplify the presentation, we write:

$$R \triangleq \square_{i=1}^n \bar{q}, |i\rangle \rightarrow P_i,$$

and assume that $\lceil P_i \rceil$ is the operator-valued function over Δ_i such that $\lceil P_i \rceil(\delta_i) = E_{i\delta_i}$ for each $\delta_i \in \Delta_i$. Let $|\psi\rangle \in \mathcal{H}_{\bigcup_{i=1}^n \text{qvar}(P_i)}$ and $|\varphi\rangle \in \mathcal{H}_{\bar{q}}$. We can write:

$$|\varphi\rangle = \sum_{i=1}^n \alpha_i |i\rangle$$

for some complex numbers α_i ($1 \leq i \leq n$). Then for any $\delta_i \in \Delta_i$ ($1 \leq i \leq n$), we have:

$$\begin{aligned} |\Psi_{\delta_1 \dots \delta_n}\rangle &\triangleq \lceil R \rceil(\oplus_{i=1}^n \delta_i)(|\psi\rangle) \\ &= \lceil R \rceil(\oplus_{i=1}^n \delta_i) \left(\sum_{i=1}^n \alpha_i |\psi i\rangle \right) \\ &= \sum_{i=1}^n \alpha_i \left(\prod_{k \neq i} \lambda_{k\delta_k} \right) E_{i\sigma_i} |\psi\rangle |i\rangle \end{aligned}$$

where $\lambda_{i\delta_i}$'s are defined as in Eq. (13),

$$|\Psi_{\delta_1 \dots \delta_n}\rangle \langle \Psi_{\delta_1 \dots \delta_n}| = \sum_{i,j=1}^n \alpha_i \alpha_j^* \left(\prod_{k \neq i} \lambda_{k\delta_k} \right) \left(\prod_{k \neq j} \lambda_{k\delta_k} \right) E_{i\delta_i} |\psi\rangle \langle \psi| E_{j\delta_j}^\dagger \otimes |i\rangle \langle j|,$$

and it follows that

$$\begin{aligned} & \text{tr}_{\mathcal{H}_{\overline{q}}} |\Psi_{\delta_1 \dots \delta_n}\rangle \langle \Psi_{\delta_1 \dots \delta_n}| \\ &= \sum_{i=1}^n |\alpha_i|^2 \left(\prod_{k \neq i} \lambda_{k\delta_k} \right)^2 E_{i\delta_i} |\psi\rangle \langle \psi| E_{i\delta_i}^\dagger. \end{aligned}$$

Using Eq. (20), we obtain:

$$\begin{aligned} & \text{tr}_{\mathcal{H}_{\overline{q}}} [\![R]\!] (|\psi\rangle \langle \psi|) \\ &= \text{tr}_{\mathcal{H}_{\overline{q}}} \left(\sum_{\delta_1, \dots, \delta_n} |\Psi_{\delta_1 \dots \delta_n}\rangle \langle \Psi_{\delta_1 \dots \delta_n}| \right) \\ &= \sum_{\delta_1, \dots, \delta_n} \text{tr}_{\mathcal{H}_{\overline{q}}} |\Psi_{\delta_1 \dots \delta_n}\rangle \langle \Psi_{\delta_1 \dots \delta_n}| \\ &= \sum_{i=1}^n |\alpha_i|^2 \left[\sum_{\delta_1, \dots, \delta_{i-1}, \delta_{i+1}, \dots, \delta_n} \left(\prod_{k \neq i} \lambda_{k\delta_k} \right)^2 \right] \\ & \quad \cdot \left[\sum_{\delta_i} E_{i\delta_i} |\psi\rangle \langle \psi| E_{i\delta_i}^\dagger \right] \\ &= \sum_{i=1}^n |\alpha_i|^2 [\![P_i]\!] (|\psi\rangle \langle \psi|). \end{aligned} \tag{23}$$

Now we do spectral decomposition for $[\![P]\!](\rho)$ and assume that

$$[\![P]\!](\rho) = \sum_l s_l |\varphi_l\rangle \langle \varphi_l|.$$

We further write:

$$|\varphi_l\rangle = \sum_i \alpha_{li} |i\rangle$$

for every l . For any density operator σ in $\mathcal{H}_{\bigcup_{i=1}^n \text{qvar}(P_i)}$, we can write σ in the form of

$$\sigma = \sum_m r_m |\psi_m\rangle \langle \psi_m|.$$

Then using Eq. (23), we get:

$$\begin{aligned}
& \llbracket \mathbf{begin\ local\ } \bar{q} := \rho; \square_{i=1}^n P, |i\rangle \rightarrow P_i \mathbf{end} \rrbracket(\sigma) \\
&= tr_{\mathcal{H}_{\bar{q}}} \llbracket P; R \rrbracket(\sigma \otimes \rho) \\
&= tr_{\mathcal{H}_{\bar{q}}} \llbracket R \rrbracket(\sigma \otimes \llbracket P \rrbracket(\rho)) \\
&= tr_{\mathcal{H}_{\bar{q}}} \llbracket R \rrbracket \left(\sum_{m,l} r_m s_l |\psi_m \varphi_l\rangle \langle \varphi_l \psi_m| \right) \\
&= \sum_{m,l} r_m s_l tr_{\mathcal{H}_{\bar{q}}} \llbracket R \rrbracket(|\psi_m \varphi_l\rangle \langle \varphi_l \psi_m|) \\
&= \sum_{m,l} r_m s_l \sum_{i=1}^n |\alpha_{li}|^2 \llbracket P_i \rrbracket(|\psi_m\rangle \langle \psi_m|) \\
&= \sum_l \sum_{i=1}^n s_l |\alpha_{li}|^2 \llbracket P_i \rrbracket \left(\sum_m r_m |\psi_m\rangle \langle \psi_m| \right) \\
&= \sum_l \sum_{i=1}^n s_l |\alpha_{li}|^2 \llbracket P_i \rrbracket(\sigma) \\
&= \sum_{i=1}^n \left(\sum_l s_l |\alpha_{li}|^2 \right) \llbracket P_i \rrbracket(\sigma) \\
&= \left\llbracket \sum_{i=1}^n P_i @ p_i \right\rrbracket(\sigma),
\end{aligned}$$

where

$$\begin{aligned}
p_i &= \sum_l s_l |\alpha_{li}|^2 = \sum_l s_l \langle i | \varphi_l \rangle \langle \varphi_l | i \rangle \\
&= \langle i | \left(\sum_l s_l |\varphi_l\rangle \langle \varphi_l| \right) | i \rangle = \langle i | \llbracket P \rrbracket(\rho) | i \rangle.
\end{aligned}$$